REMARKS

In view of the above amendments and the following remarks, reconsideration of the present application is respectfully requested.

It is noted that Claims 1-12 and 17-31 are currently pending in this application.

The Applicants wish to thank Examiner Aravind K. Moorthy for conducting another personal interview with the Applicants' representatives on April 19, 2006 at the United States Patent and Trademark Office. During the personal interview, the Applicants' representative set forth arguments clearly distinguishing each of the independent Claims 1, 11, 12, 17, 19 and 21-23 over the prior art relied upon by the Examiner. It is noted that, as reflected in the Interview Summary form PTO-413, the Examiner indicated that he would consider the Applicant's arguments upon filing of this formal response. Moreover, as also reflected in the Interview Summary form PTO-413, the Examiner suggested amendments to the independent claims to further describe how the scrambled access information is used in the challenge-response protocol in order to more clearly distinguish the present invention over the prior art. Included next is a "Substance of the Interview" including arguments presented during the personal interview for distinguishing each of independent claims 1, 11, 12, 17, 19 and 21-23 over the prior art.

It is noted that the Examiner has rejected each of independent Claims 1, 11, 12, 17, 19, and 21-23 under 35 U.S.C. § 103(a) as being unpatentable over *Candelore et al.* (U.S. Patent No. 6,061,449) in view of *Yatsukawa* (USPN: 6,148,404) for the reasons contained in Paragraph 6 on Pages 2-6 of the Office Action.

Without intending to acquiesce to the Examiner's aforementioned rejection and in order to now clearly place this application in condition for allowance, the Applicants have amended each of independent claims 1, 11, 12, 17, 19 and 21-23 as suggested by the Examiner to further

describe how the scrambled access information is used in the challenge-response protocol in order to more clearly distinguish the claims over the prior art.

Accordingly, the Applicants submit that each of newly amended independent Claims 1, 11, 12, 17, 19 and 21-23 are clearly patentably distinguished over the prior art references relied upon by the Examiner for at least the following reasons.

According to an embodiment of the present invention as now recited in each of independent claims 1, 11, 12, 17, 19 and 21-23, the access device transmits to the storage medium scrambled access information generated by scrambling access information which shows the area, and authenticates whether the storage medium is authorized according to a challenge-response authentication protocol in which first and second response values are compared, the scrambled access information being used by the access device and the storage medium for calculating the first and second response values, respectively.

For example, in the illustrative embodiment shown in Figs. 2 and 4 of the present application, the access device 10 transmits to the storage medium 20 scrambled access information R1 generated by scrambling access information which shows the area, and authenticates whether the storage medium 20 is authorized according to a challenge-response protocol in which a first response value V2' and a second response value V2 are compared, the scrambled access information R1 being used by the access device 10 and the storage medium 20 for calculating the first response value V2' = F1(R1, UK) and second response value V2 = F1(R1, UK), respectively (see Figs. 2 and 4 and paragraphs [0033] and [0053] – [0056]).

Accordingly, mutual authentication is performed very securely and effectively by using the scrambled access information in both the access device and the storage device for calculating first and second response values, respectively, and then comparing the first and second response

values. Moreover, the reading/writing of data can be quickly performed after successful authentication since the access information showing the area in the storage medium was previously used during authentication and is readily available at the outset of such reading/writing of data.

The Applicants submit that the aforementioned features, which are contained within each of newly amended independent Claims 1, 11, 12, 17, 19, and 21-23 of the present application, are not disclosed or suggested by either the *Candelore et al.* or *Yatsukawa* references.

The *Candelore et al.* reference discloses the transmission of program information in block chains from an external memory 110 to block buffers 130, 132, 134 of a descrambling receiver 100 [see Figure. 1, abstract and Column 19 (Lines 60-64)]. As clearly shown in Figures 2 and 3 and as clearly discussed in Column 26 (Lines 64-66), address data (i.e., "high address" and "low address") is used in an encryption/decryption circuit 120 to unscramble a cipher block chain sequence [see Figs. 2 and 3 Column 26 (Lines 64-66)]. After the blocks have been decrypted/encrypted using such address data, the blocks are then subjected to authentication using an authentication circuit 125 [see Figs. 2 and 3 and Column 27 (Lines 9-13)]. Accordingly, it is very evident from at least Figs. 2 and 3 of the *Candelore et al.* reference that, while such address data is used for encryption/decryption purposes, it is clearly not used for authentication [see Figs. 2 & 3].

Moreover, according to an embodiment of the present invention as now clearly recited in each of newly amended independent claims 1, 11, 12, 17, 19, and 21-23, the scrambled access information showing the area is used by both the access device and the storage medium for calculating first and second response values, respectively, which are compared for authentication. It is strongly submitted that the *Candelore et al.* reference fails to disclose using

access information showing the area in both the descrambling receiver 100 and the external memory 110 for calculating first and second response values, respectively, which are then compared for authentication.

The *Yatsukawa* reference also fails to teach or suggest the aforementioned shortcomings of the *Candelore et al.* reference.

Accordingly, Applicants submit that the *Candelore et al.* and *Yatsukawa et al.* references, taken either alone or in combination, fail to disclose or suggest that the access device transmits to the storage medium scrambled access information generated by scrambling access information which shows the area, and authenticates whether the storage medium is authorized according to a challenge-response authentication protocol in which first and second response values are compared. The scrambled access information being used by the access device and the storage medium for calculating the first and second response values, respectively, as now claimed in each of newly amended independent Claims 1, 11, 12, 17, 19 and 21-23 of the present application.

Next, according to an embodiment of the present invention as recited in each of independent Claims 1, 11, 12, 17, 19, and 21-23, when the storage medium and the access device have authenticated each other as authorized devices, the storage medium extracts the access information from the scrambled access information that was used in the authentication protocol, and the access device reads/writes digital information from/into the area shown by the access information. Accordingly, the reading/writing of the digital information from/into the area shown by the access information is performed when the storage medium and the access device successfully authenticate each other as authorized devices.

On the contrary, the *Candelore et al.* system does not perform mutual authentication for the descrambling receiver 100 and the external memory 110. Instead, the *Candelore et al.* system first transfers data between the devices, a block at a time or a chain at a time, and then subsequently performs authentication on the data itself on a block-by-block or chain-by-chain basis [see Abstract and Column 19 (Lines 60-64)].

The Applicants submit that the *Yatsukawa* reference clearly fails to teach or suggest the aforementioned shortcomings of the *Candelore et al.* reference.

Accordingly, it is submitted that the *Candelore et al.* and *Yatsukawa et al.* references, taken either alone or in combination, fail to disclose or suggest that, when the storage medium and the access device have authenticated each other as authorized devices, the storage medium extracts the access information from the scrambled access information that was used in the authentication protocol, and the access device reads/writes digital information from/into the area shown by the access information, as claimed in each of independent Claims 1, 11, 12, 17, 19 and 21-23 of the present application..

Lastly, it is noted that the Examiner has relied on the *Yatsukawa* reference merely for disclosing a challenge-response authentication protocol [see page 3 of the Office Action]. As an alleged motivation for combining the *Candelore et al.* and *Yatsukawa* references, the Examiner has stated on page 4 of the Office Action that, "It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified *Candelore et al.* by the teaching of *Yatsukawa* because the challenge-response scheme has an advantage in that even if a third person wiretaps the message, reusing the message is impossible because the challenge changes each time [Column 3, Lines 48-55].

The Applicants respectfully disagree with and traverse the Examiner's combination of the *Candelore et al.* and *Yatsukawa* reference and submit that it would not have been obvious to a person having ordinary skill in the art at the time of the invention to implement the challenge-response protocol of the *Yatsukawa* reference into the *Candelore et al.* teaching.

Particularly, as recited in Line 5 of the Abstract of the *Candelore et al.* reference, the program information is communicated in block chains to reduce the overhead of the authentication information (see Abstract). The implementation of the challenge-response protocol taught by the *Yatsukawa* reference into the *Candelore et al.* system, in the manner suggested by the Examiner, such that the challenge changes each time would increase the necessary authentication information since the challenge-response protocol would be required to be repetitively performed for each block on a block-by-block basis, thereby defeating the objective of reducing the overhead of authentication information.

In view of the foregoing, it is submitted that each of independent Claims 1, 11, 12, 17, 19, and 21-23, as well as Claims 2-10, 18, 20, and 24-31 dependent thereon, is now clearly allowable, and the Examiner is kindly requested to now promptly pass this case to issuance.

Patent
42478-8700

As discussed during the personal interview, due to the fact that four Office Actions have now been issued in this application, the Examiner is kindly requested to contact Dhiren Odedra (telephone number (202) 912-3800) in the event that the Examiner feels this application is not in condition for allowance.

I hereby certify that this correspondence is being transmitted via facsimile to the USPTO at 571-273-8300 on April 28, 2006.

By: Sharon Farnus

Sharon Farnus

Signature

Dated: April 28, 2006

Very truly yours,

SNELL & WILMER L.L.P.

Joseph W. Price
Registration No. 25,124
600 Anton Boulevard, Suite 1400
Costa Mesa, California 92626-7689
Telephone: (714) 427-7420
Facsimile: (714) 427-7799